The New FISMA Standards and Guidelines

Changing the Dynamic of Information Security for the Federal Government

Ron S. Ross, Ph.D
Computer Security Division
National Institute of Standards and Technology

The Federal Information Security Management Act (FISMA) of 2002 places significant requirements on Federal agencies for the protection of information and information systems. In response to this important legislation, the National Institute of Standards and Technology (NIST) is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. This high priority project includes the development of security categorization standards, standards and guidelines for the specification, selection, and testing of security controls for information systems, and guidelines for the certification review and accreditation of information systems. The flagship standard among those being developed by NIST is Federal Information Processing Standards (FIPS) Publication 199, *Standards for the Security Categorization of Federal Information and Information Systems*. This new mandatory standard, applicable to non-national security systems as defined by FISMA, will introduce some significant changes in how the United States Government protects its information and information systems including those systems that comprise the nation's critical infrastructure.

To gauge the importance and potential impact of FIPS Publication 199 on the massive inventory of Federal information systems, one must first understand how the world of information technology has changed over the past two decades. Not too many years ago, the information systems that populated Federal enterprises consisted of large, expensive, standalone mainframes, taking up a significant amount of physical space in the facilities and consuming substantial portions of organizational budgets. Information systems during those times were viewed as "big ticket items" requiring specialized policies and procedures to effectively manage. Today, information systems are more powerful, less costly (for the equivalent computational capability), networked, and ubiquitous. The systems, in most cases, are viewed by agencies as commodity items—albeit items coupled more tightly than ever to the accomplishment of agency missions. However, as the technology raced ahead and brought a new generation of information systems into the Federal government with new access methods and a growing community of users, some of the policies, procedures, and approaches employed to ensure the protection of those systems did not keep pace.

The Problem with the Old Way of Doing Business

Abraham Lincoln once said, "You can fool some of the people all of the time and all of the people some of the time, but you cannot fool all of the people all of the time". The spirit of this quote can be applied appropriately to today's world of high technology in the methods used to protect agency information and information systems (including missions supported and services provided). The administrative and technological costs of offering a high degree of protection for all Federal information systems at all times would be prohibitive, especially in times of tight governmental budgets. Achieving adequate, cost-effective information system security (as defined in Office of Management and Budget Circular A-130, Appendix III) in an era where information technology is a commodity requires some fundamental changes in how the protection problem is addressed. *Information systems must be assessed to establish priorities based on the importance of those systems to agency missions*.

There is clearly a criticality and sensitivity continuum with regard to agency information systems that affects the ultimate prioritization of those systems. At one end of the continuum, there are high-priority information systems performing very sensitive, mission-critical operations, perhaps

as part of the critical information infrastructure. At the other end of the continuum, there are low-priority information systems performing routine agency operations. The application of safeguards and countermeasures (i.e., security controls) to all these information systems should be tailored to the individual systems based on established agency priorities, (i.e., where the systems fall on the continuum of criticality/sensitivity with regard to supporting the agency's missions). The level of effort dedicated to testing and evaluating the security controls in Federal information systems and the determination and acceptance of risk to the mission in operating those systems (i.e., security certification and accreditation) should also be based on the same agency priorities. Until recently, there were a limited number of standards and guidelines available to help agencies implement a more granular approach to establishing security priorities for their information systems. The result—many agencies would end up expending too many resources (both administratively and technologically) to protect information systems of lesser criticality/sensitivity and not enough resources to protect systems of greater criticality/sensitivity. Some "load balancing" was needed.

Ushering in a New Era with FIPS Publication 199

FIPS Publication 199, the mandatory Federal security categorization standard recently approved by the Secretary of Commerce, provides the first step toward bringing some order and discipline to the challenge of protecting the large number of information systems supporting the operations and assets of the Federal government. The standard is predicated on a simple and well-established concept—determining appropriate priorities for agency information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the system's criticality and sensitivity. FIPS Publication 199 assigns this level of criticality and sensitivity based on the potential impact on agency operations (mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security due to the loss of confidentiality (i.e., unauthorized disclosure of information), integrity (i.e., unauthorized modification of information), or availability (i.e., denial of service). FIPS Publication 199 requires Federal agencies to do a "triage" on all of their information types and systems, categorizing each as low, moderate, or high impact for the three security objectives of confidentiality, integrity (including authenticity and non-repudiation), and availability.

Employed within the System Development Life Cycle (SDLC), FIPS Publication 199 can be used as part of an agency's risk management program to help ensure that appropriate security controls are applied to each information system and that the controls are adequately assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The following activities, consistent with **NIST Special Publication 800-30**, *Risk Management Guide for Information Technology Systems*, can be applied to both new and legacy information systems within the SDLC—

- ***Categorize*** the information system (and the information resident within that system) based on a FIPS Publication 199 impact analysis (See **NIST Special Publication 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance in assigning security categories and refining the impact analysis).
- ***Select*** an initial set of security controls for the information system (as a starting point) based on the FIPS Publication 199 security categorization (See **NIST Special Publication 800-53**, *Recommended Security Controls for Federal Information Systems*).[1]

[1] **FIPS Publication 200**, *Security Controls for Federal Information Systems*, will replace NIST Special Publication 800-53 in December 2005 in fulfillment of the FISMA legislative requirement for mandatory minimum security requirements for Federal information systems.

- ***Refine*** the initial set of security controls selected for the information system based on local conditions including agency-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or other special circumstances.
- ***Document*** the agreed upon set of security controls in the system security plan including the agency's rationale and justification for any refinements or adjustments to the initial set of controls (See **NIST Special Publication 800-18**, *Guide for Developing Security Plans for Information Technology Systems*).
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (See **NIST Special Publication 800-53A**, *Guide for Assessing the Security Controls in Federal Information Systems*, Summer 2004).[2]
- ***Determine*** the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the planned or continued operation of the information system (See **NIST Special Publication 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*).
- ***Authorize*** system processing (or for legacy systems, authorize continued system processing) if the level of risk to the agency's operations, assets, or individuals is acceptable to the authorizing official (See **NIST Special Publication 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*).
- ***Monitor*** selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate agency officials on a regular basis (See **NIST Special Publication 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*).

Significant changes to the information system or the security requirements for that system may prompt the agency to revisit the above activities.[3]

The Benefits to Agency Security Programs

The long-term effect of employing a FIPS Publication 199 standards-based approach is better, more targeted, and cost-effective security for Federal information and information systems. While the interconnection of information systems often increases the risk to an agency's operations and assets, FIPS Publication 199 and the associated suite of standards and guidelines, provides a common framework and understanding for expressing information security, and thus promotes greater consistency across diverse organizations in managing that risk. Agencies will determine which information systems are the most important to accomplishing assigned missions based on the security categorization of those systems and will protect the systems appropriately. Agencies will also determine which systems are the least important to their missions and will not allocate

[2] The determination of security control effectiveness during the assessment process may require remedial actions such as employing additional controls or fixing controls that are ineffective. See NIST Special Publication 800-53.

[3] A significant change is typically defined as any change to the hardware, software, or firmware components of an information system that may have an impact on the protection capabilities of that system and the enforcement of the system security policy. Examples include such things as the installation of a new or upgraded operating system, firewall, database management system, network device, or identification and authentication mechanism.

excessive resources for the protection of those systems. In the current high technology era where information systems are viewed as commodities and are routinely used to protect some of the nation's most important assets within the Federal government and the critical infrastructure, FIPS Publication 199 is a standard that is right for the time. In the end, the new security standard, when properly applied, will facilitate a more effective allocation of available resources for protecting information systems, determine the need and provide a justification for the allocation of additional resources, and result in a substantial improvement in the security posture of the government's information systems.[4]

[4] The FISMA-related security standards and guidelines discussed in this article are available at the FISMA Implementation Project web site at http://csrc.nist.gov/sec-cert.